BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT/JP01/00159
09/936157
12.01.01

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JP01/159

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

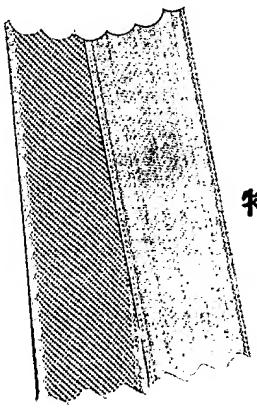
出願年月日
Date of Application: ２０００年　１月１４日

EKU

出願番号
Application Number: 特願２０００－００６９８９

出願人
Applicant (s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



２００１年　２月１６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３００７２８４

【書類名】　特許願

【整理番号】　2022520013

【提出日】　平成12年 1月14日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L　9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　柴田　修

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　湯川　泰平

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　関部　勉

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　廣田　照人

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　齊藤　義行

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大竹　俊彦

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【選任した代理人】

【識別番号】　100109210

【弁理士】

【氏名又は名称】　新居　広守

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9810105

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証通信装置およびシステム

【特許請求の範囲】

【請求項１】　共通鍵を用いて暗号通信を行うリードライタ装置あるいはメモリ装置であって、

前記リードライタ装置は、

共通鍵を記憶する第１共通鍵記憶手段と、

アクセス情報を記憶するアクセス情報記憶手段と、

乱数種を記憶する第１乱数種記憶手段と、

前記アクセス情報記憶手段に格納されているアクセス情報と前記第１乱数種記憶手段に格納されている乱数種とを合成する合成処理手段と、

前記合成処理手段で合成されたデータを前記第１共通鍵記憶手段に格納されている共通鍵を用いて暗号化して第１乱数を生成する暗号化手段と、

前記暗号化手段で生成した第１乱数を前記第１乱数種記憶手段に格納する第１乱数種更新手段と、

前記暗号化手段で生成した第１乱数と前記メモリ装置から転送される第２乱数を用いて前記メモリ装置と相互認証を行なう第１相互認証処理手段と、

前記第１相互認証処理手段における認証受理をうけて前記暗号化手段で生成した前記第１乱数と前記メモリ装置から転送される第２乱数から時変鍵を生成する第１時変鍵生成手段と、

前記リードライタ装置の機密データを前記第１時変鍵生成手段で生成された時変鍵を用いて暗号化して暗号化機密データを生成し前記メモリ装置に転送する、

あるいは前記メモリ装置から転送される暗号化機密データを前記第１時変鍵生成手段で生成された時変鍵を用いて復号化して機密データを抽出する第１暗号復号化手段を具備することを特徴とする認証通信装置、

あるいは前記メモリ装置は、

機密データを記憶する機密データ記憶手段と、

共通鍵を記憶する第２共通鍵記憶手段と、

乱数種を記憶する第２乱数種記憶手段と、

前記リードライタ装置から転送される第１乱数を前記第２共通鍵記憶手段に格納されている共通鍵を用いて復号化する復号化手段と、

前記第１復号手段で復号化したデータからアクセス情報を分離する分離処理手段と、

前記第２乱数種記憶手段に格納されている乱数種から第２乱数を生成する乱数生成手段と、

前記乱数生成手段で生成した第２乱数を前記第２乱数種記憶手段に格納する第２乱数種更新手段と、

前記リードライタ装置から転送される第１乱数と前記乱数生成手段で生成した第２乱数を用いて前記リードライタ装置と相互認証を行なう第２相互認証処理手段と、

前記第２相互認証処理手段における認証受理をうけて前記リードライタ装置から転送される第１乱数と前記乱数生成手段で生成した第２乱数から時変鍵を生成する第２時変鍵生成手段と、

前記分離処理手段から分離されたアクセス情報を基に前記機密データ記憶手段に格納されている情報から機密データを選択し前記第２時変鍵生成手段で生成された時変鍵を用いて暗号化して暗号化機密データを生成し前記リードライタ装置に転送する、

あるいは前記リードライタ装置から転送される暗号化機密データを前記第２時変鍵生成で生成された時変鍵を用いて復号化して機密データを抽出し前記分離処理手段から分離されたアクセス情報を基に前記機密データ記憶手段に格納する第２暗号復号化手段を具備することを特徴とする認証通信装置、

および前記リードライタ装置および前記メモリ装置を有することを特徴とする認証通信システム。

【請求項２】　共通鍵を用いて暗号通信を行うリードライタ装置あるいはメモリ装置であって、

前記リードライタ装置は、

共通鍵を記憶する第１共通鍵記憶手段と、

アクセス情報を記憶するアクセス情報記憶手段と、

乱数種を記憶する第１乱数種記憶手段と、

前記第１乱数種記憶手段に格納されている乱数種から第３乱数を生成する第１乱数生成手段と、

前記アクセス情報記憶手段に格納されているアクセス情報と前記第１乱数種生成手段で生成された第３乱数とを合成する合成処理手段と、

前記合成処理手段で合成されたデータを前記第１共通鍵記憶手段生成に格納されている共通鍵を用いて暗号化して第１乱数を生成する暗号化手段と、

前記第１乱数化手段で生成した第３乱数を前記第１乱数種記憶手段に格納する第１乱数種更新手段と、

前記暗号化手段で生成した第１乱数と前記メモリ装置から転送される第２乱数を用いて前記メモリ装置と相互認証を行なう第１相互認証処理手段と、

前記第１相互認証処理手段における認証受理をうけて前記暗号化手段で生成した第１乱数と前記メモリ装置から転送される第２乱数から時変鍵を生成する第１時変鍵生成手段と、

前記リードライタ装置の機密データを前記第１時変鍵生成手段で生成された時変鍵を用いて暗号化して暗号化機密データを生成し前記メモリ装置に転送する、

あるいは前記メモリ装置から転送される暗号化機密データを前記第１時変鍵生成手段で生成された時変鍵を用いて復号化して機密データを抽出する第１暗号復号化手段を具備することを特徴とする認証通信装置、

あるいは前記メモリ装置は、

機密データを記憶する機密データ記憶手段と、

共通鍵を記憶する第２共通鍵記憶手段と、

乱数種を記憶する第２乱数種記憶手段と、

前記リードライタ装置から転送される第１乱数を前記第２共通鍵記憶手段に格納されている共通鍵を用いて復号化する復号化手段と、

前記第１復号手段で復号化したデータからアクセス情報を分離する分離処理手段と、

前記第２乱数種記憶手段に格納されている乱数種から第２乱数を生成する第２乱数生成手段と、

前記第２乱数生成手段で生成した第２乱数を前記第２乱数種記憶手段に格納する第２乱数種更新手段と、

前記リードライタ装置から転送される第１乱数と前記第２乱数生成手段で生成した第２乱数を用いて前記リードライタ装置と相互認証を行なう第２相互認証処理手段と、

前記第２相互認証処理手段における認証受理をうけて前記リードライタ装置から転送される第１乱数と前記乱数生成手段で生成した第２乱数から時変鍵を生成する第２時変鍵生成手段と、

前記分離処理手段から分離されたアクセス情報を基に前記機密データ記憶手段に格納されている情報から機密データを選択し前記第２時変鍵生成手段で生成された時変鍵を用いて暗号化して暗号化機密データを生成し前記リードライタ装置に転送する、

あるいは前記リードライタ装置から転送される暗号化機密データを前記第２時変鍵生成で生成された時変鍵を用いて復号化して機密データを抽出し前記分離処理手段から分離されたアクセス情報を基に前記機密データ記憶手段に格納する第２暗号復号化手段を具備することを特徴とする認証通信装置、

および前記リードライタ装置および前記メモリ装置を有することを特徴とする認証通信システム。

【請求項３】　前記時変鍵生成手段が前記第１および第２乱数と前記共通鍵を用いて時変鍵を生成することを特徴とする請求項１または２記載の認証通信装置およびシステム。

【請求項４】　前記第１および第２相互認証処理手段はチャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証することを特徴とする請求項１または２または３記載の認証通信装置およびシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、音楽、画像、映像、ゲームなどのディジタルコンテンツを械器間で

共通鍵を共有化して暗号通信を行う装置およびシステムにおいて、相互認証と同時に著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスするための情報（アドレス、セクタ数など）を暗号化して転送する認証通信装置およびシステムに関する。

【０００２】

【従来の技術】

近年、ディジタル情報圧縮技術の進展とインターネットに代表されるグローバルな通信インフラの爆発的な普及によって音楽、画像、映像、ゲームなどのコンテンツをディジタル情報として通信回線を利用して各家庭に配信することが実現されはじめた。

【０００３】

ディジタルコンテンツの著作権者の権利や流通業者の利益を保護した流通配信システムを確立するために、通信の傍受、盗聴、なりすましなどによる不正入手や、受信したデータを記憶した記録媒体における違法複製、違法改ざんなどの不正行為を防止することが課題となり、正規システムの判別、データスクランブルを行なう暗号/認証などの著作物保護技術が必要となる。

【０００４】

著作物保護技術については従来より種々なものが知られており、代表的なものとして著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスする際に、機器間で乱数と応答値の交換を行なって相互に正当性を認証し合い、正当である場合のみアクセスを許可するチャレンジレスポンス型の相互認証技術がある。また、機密データを相互認証に用いた乱数あるいは応答値を用いて暗号通信を行い、不正解読を防止する。

【０００５】

【発明が解決しようとする課題】

ここで課題となるのは、著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスするための情報（アドレス、セクタ数など）の機密性をどのように保護するかである。

機密データ記憶領域にアクセスするための情報の改竄による不正行為を考えて

みると、例えば相互認証だけ正規機器を用いて行い、機密データ記憶領域にアクセスするための情報をなりすまして別の情報に改竄して転送し、機密データ記憶領域の機密データを不正に入手する行為が考えられる。

【０００６】

上記不正行為に防止するには、前述の暗号通信技術を機密データだけに適用するのではなくでなく、機密データ記憶領域にアクセスするための情報にも拡大して適用すればよい。しかし、単純に相互認証を行った後に、機密データ記憶領域にアクセスするための情報の暗号通信、機密データの暗号通信という処理にしても、機密データ記憶領域にアクセスするための情報の暗号通信方法が露呈した場合、前述の不正行為が可能となる。

【０００７】

そこで、本発明では、機密データ記憶領域にアクセスするための情報を暗号化して機密性を保護し、かつ不正に改竄された場合にアクセスできなくする装置およびシステムを提供することにある。

【０００８】

【課題を解決するための手段】

以上のような課題を解決するため、本発明は、相互認証と同時に機密データ記憶領域にアクセスするための情報を暗号化して転送する。

【０００９】

【発明の実施の形態】

以下に本発明の原理と実施例を添付の図面を用いて説明する。

（実施の形態１）

図１は、本発明の実施の形態１における構成図を示しリードライタ装置１０１とメモリ装置１０２が暗号通信を行なうシステムである。

【００１０】

両装置ともに、乱数発生に用いる乱数種を格納する乱数種記憶手段１１３、１１４、共通鍵ＵＫを格納する共通鍵記憶手段１０５、１０６を備える。なお、これら記憶手段は外部から直接アクセスすることができないプロテクト領域に記憶されており、装置製造時に乱数種の初期値と共通鍵が書き込まれる。

また、メモリ装置１０２に著作物の保護を要する機密データを格納する機密データ記憶手段１２２を備え、リードライタ装置１０１に機密データ記憶手段１２２へのアクセス情報１０３を備える。なお、アクセス情報は入出力手段１２５を介して与えられる。

【００１１】

リードライタ装置１０１がメモリ装置１０２の機密データ記憶手段１２２にアクセスするには、まず、リードライタ装置１０１のアクセス情報１０３と乱数種記憶手段１１３に格納されている乱数種とを合成処理手段１０７で合成する。ここで合成処理方法としては、例えばアクセス情報１０３のデータ長が３２ビット、乱数種のデータ長が６４ビット、合成されたデータのデータ長が６４ビットとした場合、アクセス情報１０３のデータ３２ビットと乱数種の下位データ３２ビットを連結して６４ビットの合成データを生成するようにすればよい。

【００１２】

次に、合成処理手段１０７で合成されたデータを共通鍵記憶手段１０５に格納されている共通鍵ＵＫを用いて暗号化手段１０９で暗号化して第１乱数Ｒ１を生成し、かつ乱数種更新手段１２３を用いて第１乱数Ｒ１を乱数種記憶手段１１３に格納して乱数種を更新する。メモリ装置１０２でも、乱数生成手段１１２で乱数種記憶手段１１４に格納されている乱数種から第２乱数Ｒ２を生成し、かつ乱数種更新手段１２４を用いて乱数種記憶手段１１４に格納して乱数種を更新する。その後、互いの乱数（Ｒ１、Ｒ２）を交換し、または応答値（Ｖ１、Ｖ２）を交換し比較することによって相互に相手装置が正当な装置であることを認証するチャレンジレスポンス型の相互認証（１１５、１１６）を行なう。相互認証処理手段１１５、１１６によって相手機器が正当であること確認されたら、互いの乱数（Ｒ１、Ｒ２）から相互認証毎に変化する時変鍵ＶＫを生成（１１７、１１８）し共有化する。また、メモリ装置では、同時に第１乱数Ｒ１を共通鍵記憶手段１０６に格納されている共通鍵ＵＫを用いて復号化手段１１０で復号化してアクセス情報１０３が含まれる合成データを抽出し、分離処理手段１０８でアクセス情報を分離する。

【００１３】

ここで、リードライタ装置１０１からメモリ装置１０２の機密データ記憶手段１２２に機密データ１２１を書き込む場合は、リードライタ装置１０１の時変鍵生成手段１１７で生成した時変鍵ＶＫを用いて入出力手段１２５を介して与えられる機密データ１２１を暗号化して暗号化機密データを生成してメモリ装置１０２へ転送する。メモリ装置１０２では、時変鍵生成手段１１８で生成した時変鍵ＶＫを用いて転送された暗号化機密データを復号化して機密データを得て、分離処理手段１０８で分離されたアクセス情報１０４を基に、機密データ記憶手段１２２に格納する。

【００１４】

同様に、メモリ装置１０１の機密データ記憶手段１２２に格納されている機密データをリードライタ装置１０１に読み込む場合は、メモリ装置１０２の分離処理手段１０８で分離されたアクセス情報１０４を基に、機密データ記憶手段１２２に格納されている機密データをリードし、時変鍵生成手段１１８で生成した時変鍵ＶＫを用いて機密データを暗号化して暗号化機密データを生成してリードライタ装置１０１へ転送する。リードライタ装置１０１では、時変鍵生成手段１１７で生成した時変鍵ＶＫを用いて転送された暗号化機密データを復号化して機密データを得る。

【００１５】

なお、本実施の形態では、第２乱数の生成方法は乱数生成手段で生成された乱数値を第２乱数としたが、乱数生成に用いた乱数種を第２乱数としてもよい。また、時変鍵の生成に、相互認証に用いた乱数を用いたが、応答値を用いてもかまわない。

また、アクセス情報、機密データの暗号化および復号化に用いる方法は同一のアルゴリズムのものを用いてよく、例えばＤＥＳ(Data Encryption Standard)などを用いればよい。

【００１６】

また、第２乱数、相互認証の応答値、時変鍵の生成に用いる方法は同一のアルゴリズムのものを用いてよく、例えばSHA(Secure Hash Algorithm)などの一方向性の関数を用いればよい。

また、共通鍵、時変鍵の鍵長は何ビットでもよく、例えば５６ビットとすればよい。

【００１７】

以上のように、本実施の形態の認証通信装置およびシステムは、相互認証と同時に機密データ記憶領域（手段）にアクセスするための情報を暗号化して転送するため、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。また、仮に機密データ記憶領域にアクセスするための情報を不正になりすまして別の情報に改竄して転送されると、リードライタ装置で認識している第１乱数Ｒ１とメモリ装置で認識している第１乱数Ｒ１が異なることになるので相互認証が確立しないため、機密データ記憶領域にアクセスするための情報を不正に改竄された場合、機密データ記憶領域にアクセスできなくすることが可能であり、機密データを不正に入手するのを防止できるという効果がある。

（実施の形態２）

図２は、本発明の実施の形態２における構成図を示し、図１で示した認証通信装置およびシステムにおいて、アクセス情報１０３の成分を含む第１乱数Ｒ１を乱数種更新手段１２３を用いて乱数種記憶手段１１３に格納して乱数種を更新するのではなく、メモリ装置１０２だけでなくリードライタ装置１０１にも乱数生成手段２１１を有する構成にして、乱数生成手段２１１で乱数種記憶手段１１３に格納されているアクセス情報１０３に依存しない乱数種から乱数を生成し、生成した乱数を乱数種更新手段１２３を用いて乱数種記憶手段１１４に格納して乱数種を更新するようにしたものである。

【００１８】

以上のように、本実施の形態の認証通信装置およびシステムは、乱数の更新に機密データ記憶領域にアクセスするための情報（固定値）が関連しないため、乱数の周期性を高めることができるという効果がある。

【００１９】

【発明の効果】

以上のことより本発明は以下のような効果を奏する。本発明に係る認証通信装置およびシステムは、相互認証と同時に機密データ記憶領域にアクセスするため

の情報を暗号化して転送するため、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。また、仮に機密データ記憶領域にアクセスするための情報を不正になりすまして別の情報に不正に改竄して転送されると相互認証が確立しないため、機密データ記憶領域にアクセスできなくすることが可能であり、機密データを不正に入手するのを防止できるという効果がある。

【００２０】

また、本発明に係る認証通信装置およびシステムは、乱数の更新に機密データ記憶領域にアクセスするための情報（固定値）が関連しないため、乱数の周期性を高めることができるという効果がある。

【図面の簡単な説明】

【図１】

実施の形態１の構成を示す構成図である。

【図２】

実施の形態２の構成を示す構成図である。

【符号の説明】

１０１　リードライタ装置

１０２　メモリ装置

１０３　アクセス情報記憶手段

１０４　アクセス情報

１０５、１０６　共通鍵記憶手段

１０７　合成処理手段

１０８　分離処理手段

１０９　暗号化手段

１１０　復号化手段

１１２、２１１　乱数生成手段

１１３、１１４　乱数種記憶手段

１１５、１１６　相互認証処理手段

１１７、１１８　時変鍵生成手段

１１９、１２０　暗号化復号化手段

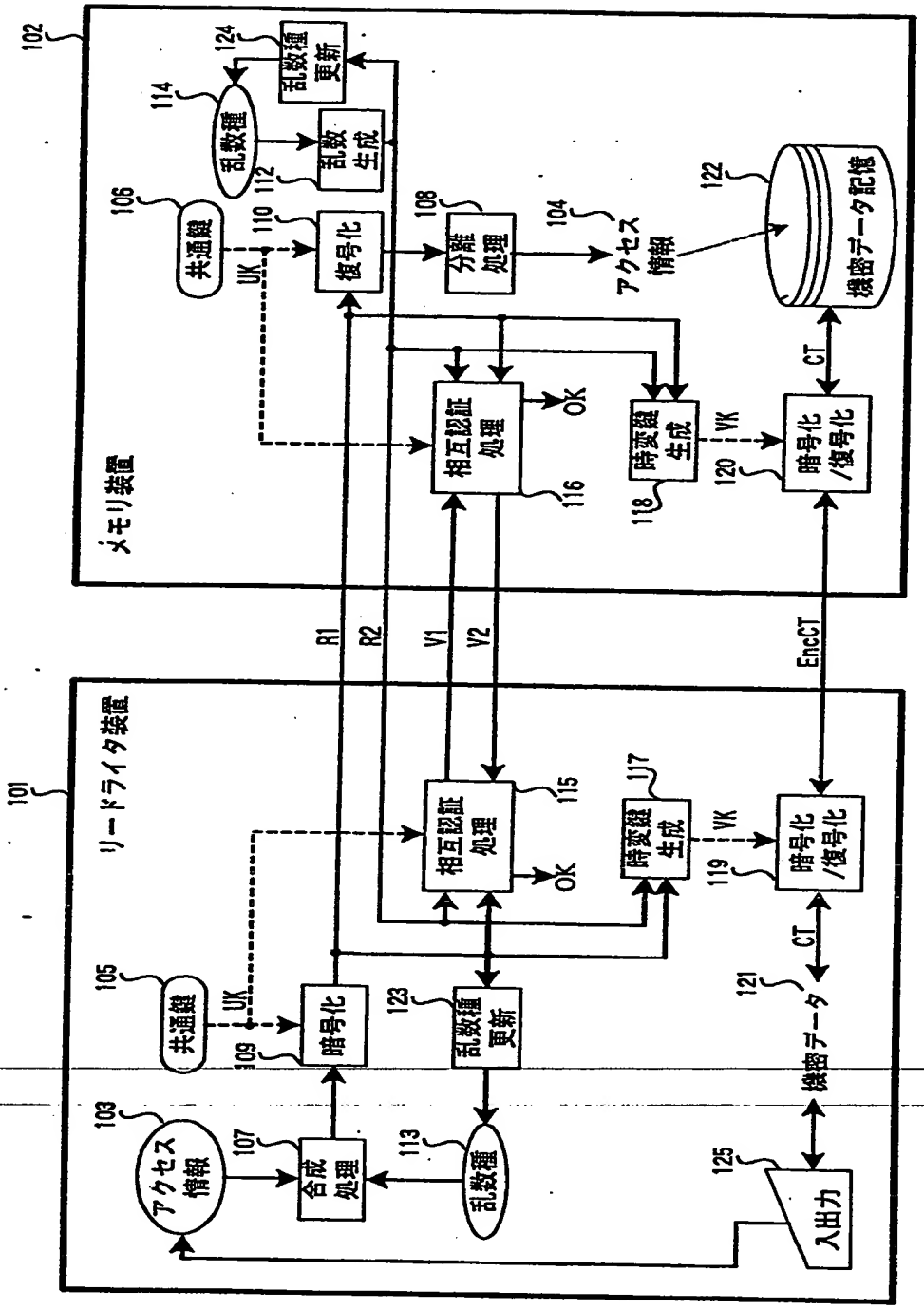
１２１　機密データ

１２２　機密データ記憶手段

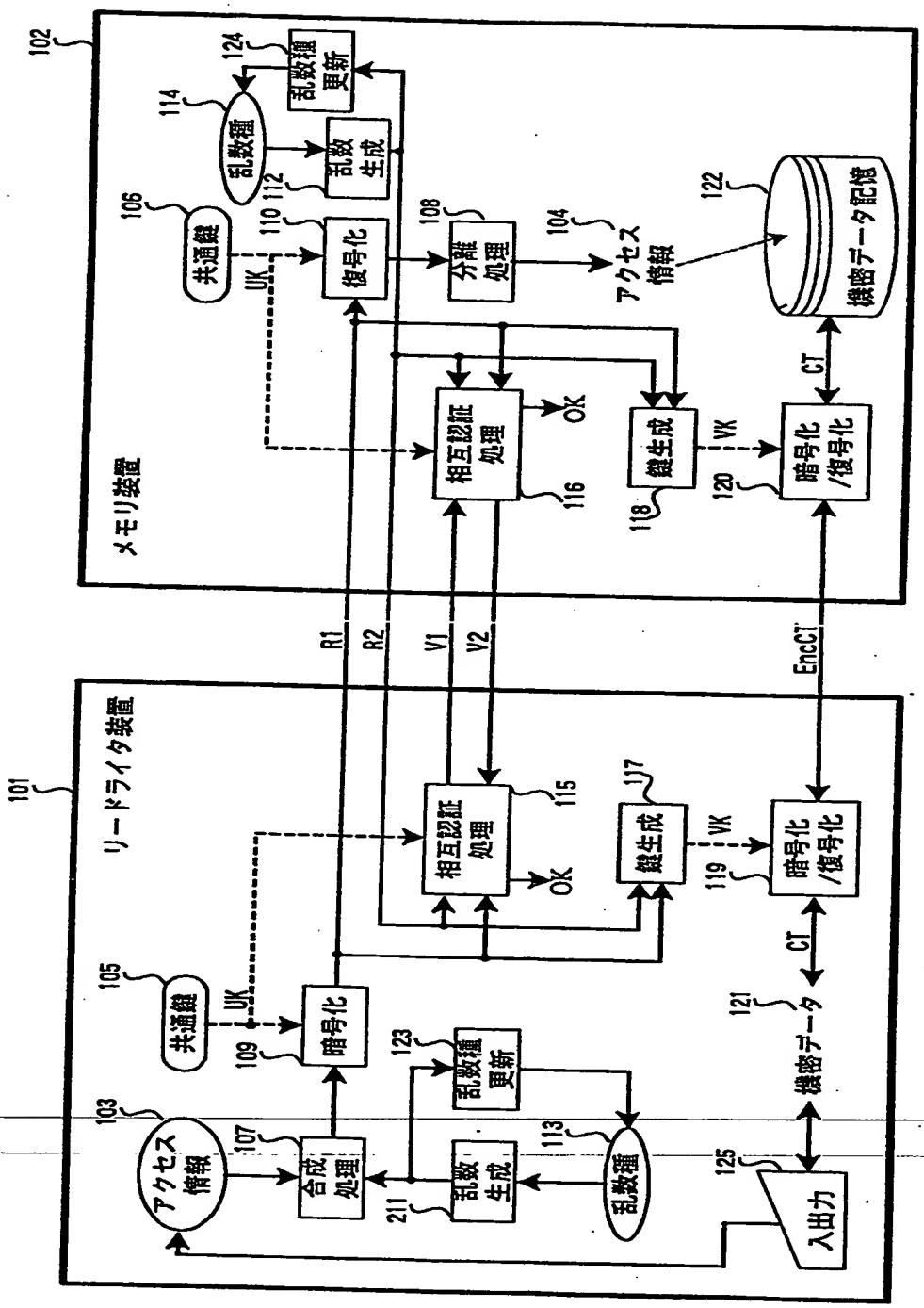
１２３、１２４　乱数種更新手段

【書類名】　　図面

【図１】


メモリ装置
リードライタ装置
乱数種 更新
乱数 生成
乱数種
共通鍵
復号化
分離 処理
アクセス 情報
機密データ記憶
相互認証 処理
時変鍵 生成
暗号化 /復号化
OK
VK
UK
CT
EncCT
R1
R2
V1
V2
合成 処理
入出力
機密データ

【図２】


メモリ装置
リードライタ装置
乱数種
乱数生成
共通鍵
復号化
分離処理
アクセス情報
機密データ記憶
相互認証処理
鍵生成
暗号化/復号化
乱数種更新
暗号化
合成処理
入出力
R1
R2
V1
V2
EncCT
CT
OK
VK
UK

【書類名】　　要約書

【要約】

【課題】　機密データが格納されている機密データ記憶領域にアクセスするための情報（アドレス，セクタ数など）の機密性を高め，かつ不正に改竄された場合に機密データ記憶領域にアクセスできなくするようにして，機密データを不正に入手することを防止する装置およびシステムを提供する。

【解決手段】　共通鍵を用いて暗号通信を行うリードライタ装置あるいはメモリ装置において、リードライタ装置及びメモリ装置はチャレンジレスポンス型の相互認証によって相手機器が正当な機器であることを認証すると同時に機密データ記憶領域にアクセスするための情報を暗号化して転送を行う構成とした。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社